Vulnerability Assessment

Per effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable, ecco una guida dettagliata su come procedere, con le fasi di configurazione, esecuzione e analisi della scansione.

Fase 1: Configurazione e avvio della scansione

1. **Installazione di Nessus**: Se non avete già installato Nessus, potete scaricarlo dal sito ufficiale di Tenable e seguire le istruzioni per l'installazione sulla vostra piattaforma.
2. **Creazione di un nuovo scan**:
   - Aprire Nessus e accedere al vostro account.
   - Cliccare su **New Scan**.
   - Selezionare il tipo di scansione: per questo esercizio potete scegliere **Basic Network Scan** o **Advanced Scan**.
   - Nella configurazione dello scan, impostare il target su **Metasploitable** e specificare solo le porte comuni. Le porte comuni possono includere: 21 (FTP), 22 (SSH), 23 (Telnet), 25 (SMTP), 80 (HTTP), 110 (POP3), 139 (NetBIOS), 143 (IMAP), 443 (HTTPS), 445 (SMB), 3306 (MySQL), 3389 (RDP), ecc.
3. **Esecuzione della scansione**:
   - Nella sezione **Targets**, inserire l'indirizzo IP della macchina Metasploitable.
   - Configurare le altre impostazioni avanzate se necessario, come la politica di autenticazione e le opzioni di scan.
   - Cliccare su **Save** e poi su **Launch** per avviare la scansione.

Fase 2: Analisi del Report

1. **Download del Report**:
   - Una volta completata la scansione, aprire il report generato da Nessus.
   - Scaricare il report in formato PDF per l'analisi.
2. **Analisi delle vulnerabilità**:
   - Per ogni vulnerabilità trovata, esaminare attentamente le seguenti informazioni:
     - **Porta e Servizio**: La porta e il servizio associato alla vulnerabilità.
     - **Descrizione della Vulnerabilità**: Tradurre in italiano se necessario.
     - **Gravità**: Valutare la criticità della vulnerabilità (bassa, media, alta, critica).
     - **Soluzione**: Tradurre e dettagliare le azioni correttive necessarie per mitigare la vulnerabilità.
3. **Approfondimento**:
   - Utilizzare i link all'interno del report di Nessus per ulteriori dettagli sulle vulnerabilità.
   - Consultare risorse online per una comprensione più approfondita, se necessario.

Esempio di Report Tecnico

Porta: 21 (FTP)

- **Descrizione**: Il servizio FTP su questa porta consente accessi anonimi.
- **Gravità**: Alta
- **Soluzione**: Disabilitare gli accessi anonimi nel file di configurazione del server FTP (solitamente `vsftpd.conf` o `proftpd.conf`). Consentire solo connessioni FTP autentificate.

Porta: 22 (SSH)

- **Descrizione**: Il servizio SSH su questa porta è vulnerabile ad attacchi brute-force a causa della mancanza di restrizioni sugli accessi.
- **Gravità**: Media
- **Soluzione**: Implementare misure di sicurezza come l'uso di chiavi SSH invece delle password, abilitare il firewall per limitare gli accessi SSH a indirizzi IP specifici, e configurare il file di configurazione SSH (`sshd_config`) per limitare il numero di tentativi di accesso.

Porta: 80 (HTTP)

- **Descrizione**: Il servizio HTTP su questa porta utilizza una versione obsoleta di Apache che contiene vulnerabilità note.
- **Gravità**: Critica
- **Soluzione**: Aggiornare il server Apache alla versione più recente disponibile. Assicurarsi di seguire le linee guida di sicurezza per la configurazione di Apache.

Consegna del Report

1. **Compilare il report in formato PDF**:
    - Includere tutte le vulnerabilità trovate, specificando la porta, la descrizione, la gravità e la soluzione.
    - Aggiungere eventuali note aggiuntive o raccomandazioni basate sull'analisi delle vulnerabilità.
2. **Inviare il report**:
    - Salvare il report in formato PDF con un nome significativo, ad esempio: `Vulnerability_Assessment_Report_Metasploitable.pdf`.
    - Condividere il PDF con il destinatario designato per la revisione.

Esempio di sezione del Report PDF

Vulnerability Assessment Report: Metasploitable

Porta: 21 (FTP)

- **Descrizione**: Il servizio FTP su questa porta consente accessi anonimi.
- **Gravità**: Alta
- **Soluzione**: Disabilitare gli accessi anonimi nel file di configurazione del server FTP (solitamente `vsftpd.conf` o `proftpd.conf`). Consentire solo connessioni FTP autentificate.

Porta: 22 (SSH)

- **Descrizione**: Il servizio SSH su questa porta è vulnerabile ad attacchi brute-force a causa della mancanza di restrizioni sugli accessi.
- **Gravità**: Media
- **Soluzione**: Implementare misure di sicurezza come l'uso di chiavi SSH invece delle password, abilitare il firewall per limitare gli accessi SSH a indirizzi IP specifici, e configurare il file di configurazione SSH (`sshd_config`) per limitare il numero di tentativi di accesso.

Porta: 80 (HTTP)

- **Descrizione**: Il servizio HTTP su questa porta utilizza una versione obsoleta di Apache che contiene vulnerabilità note.
- **Gravità**: Critica
- **Soluzione**: Aggiornare il server Apache alla versione più recente disponibile. Assicurarsi di seguire le linee guida di sicurezza per la configurazione di Apache.